

Cyber Security & Ethical Hacking Giorno 5 – Progetto

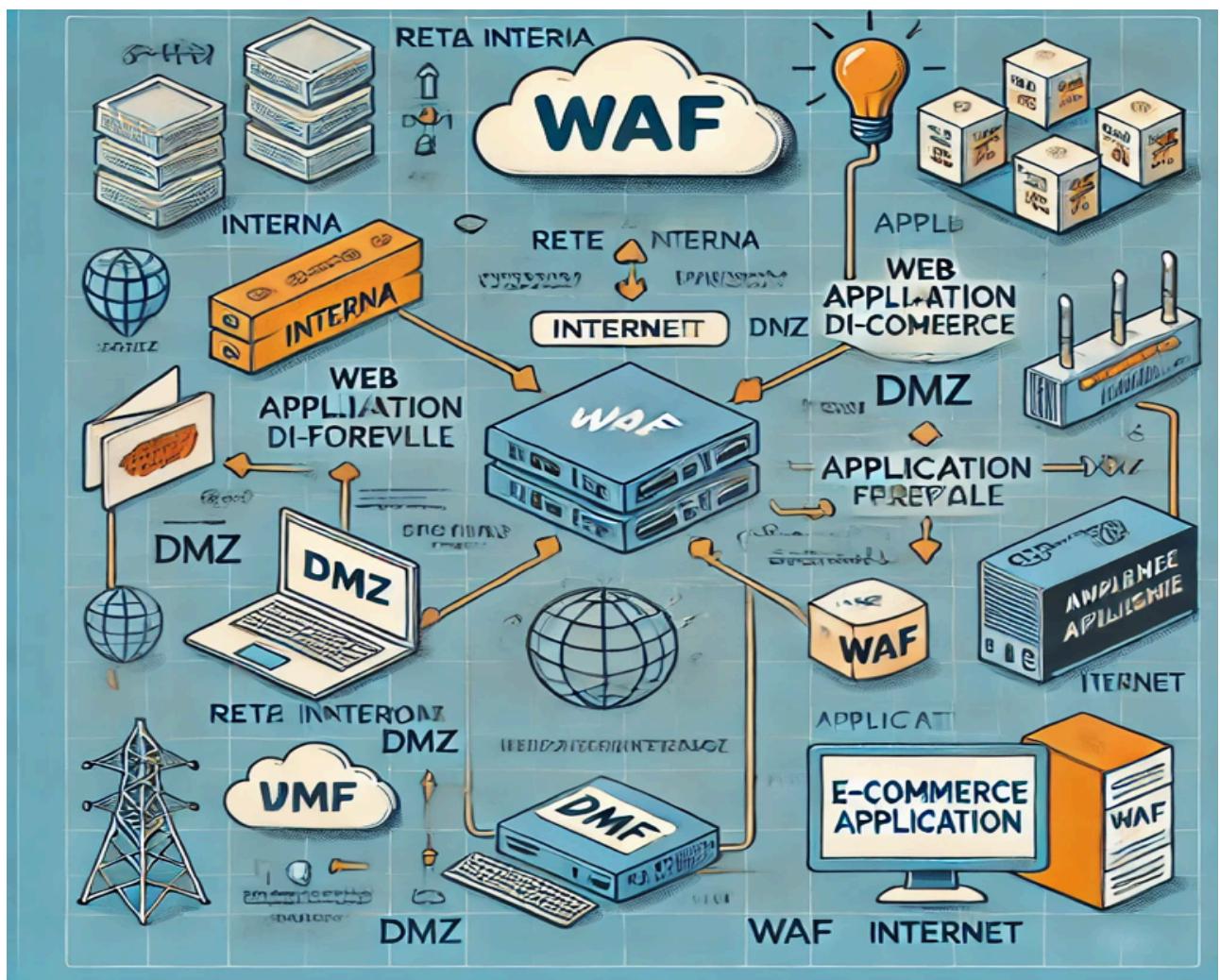
1. Azioni preventive contro SQLi e XSS

Misure preventive:

- Firewall per Applicazioni Web (WAF): Aggiungere un WAF tra Internet e l'applicazione di e-commerce. Questo può filtrare il traffico dannoso e prevenire attacchi SQLi e XSS.
- Validazione degli input: Assicurarsi che l'applicazione validi e sanifichi tutti gli input degli utenti per prevenire attacchi di iniezione.
- Aggiornamenti di sicurezza regolari: Mantenere aggiornati tutti i software e le librerie per correggere le vulnerabilità note.

Modifiche alla figura:

- Aggiungere un WAF nella DMZ per filtrare il traffico in entrata verso l'applicazione di e-commerce.



2. Impatti sul business in caso di attacco DDoS

Calcolo dell'impatto:

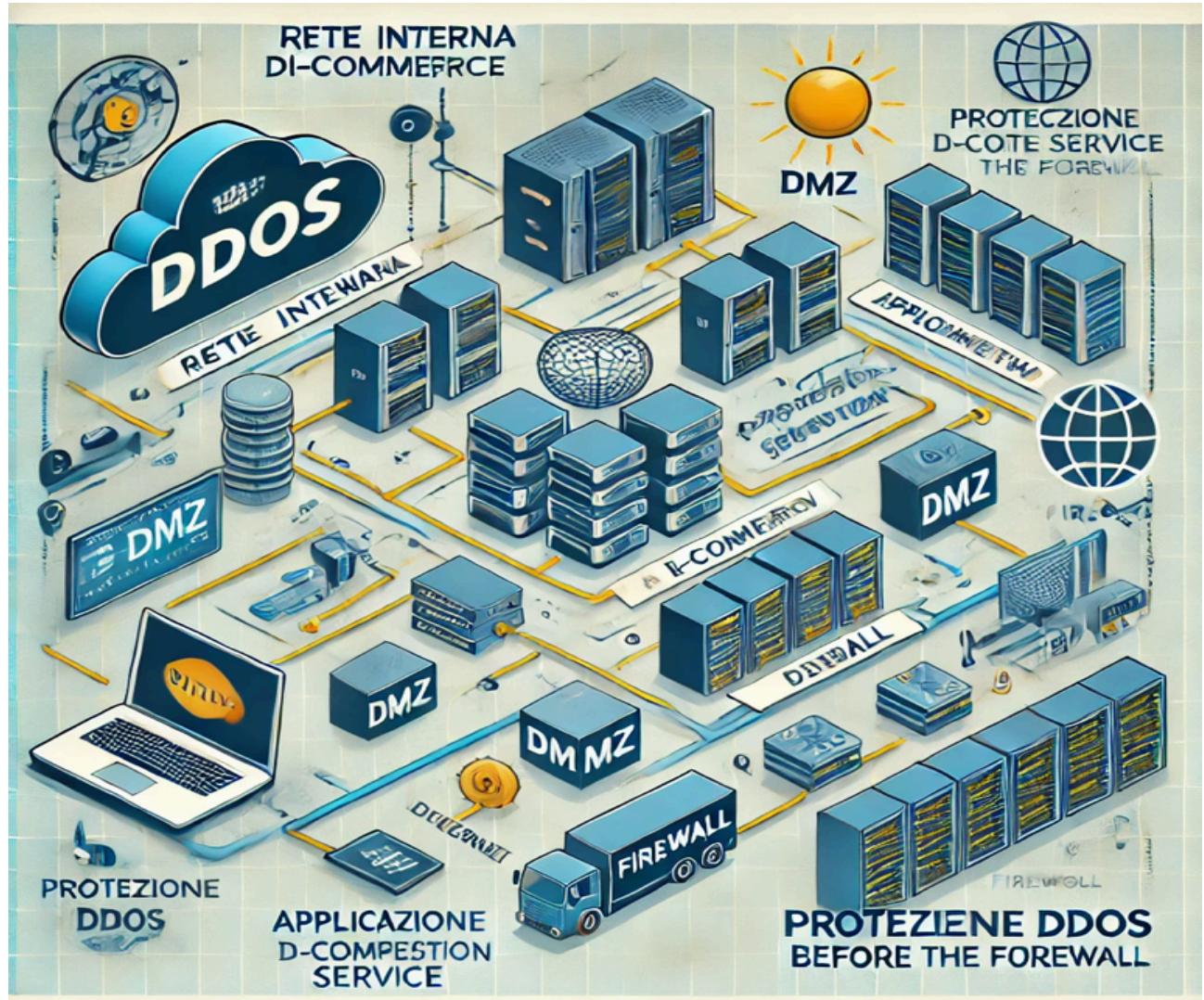
- Durata dell'attacco DDoS: 10 minuti
- Spesa media per minuto: €1500
- Impatto totale: 10 minuti * €1500/minuto =€15,000

Misure preventive per DDoS:

- Servizio di protezione DDoS: Implementare un servizio di mitigazione DDoS per assorbire e filtrare il traffico dannoso.
- Limitazione del tasso: Configurare la limitazione del tasso per gestire e mitigare eccessivi tassi di richiesta.

Modifiche alla figura:

- Aggiungere un servizio di protezione DDoS prima del firewall per assorbire e filtrare il traffico.



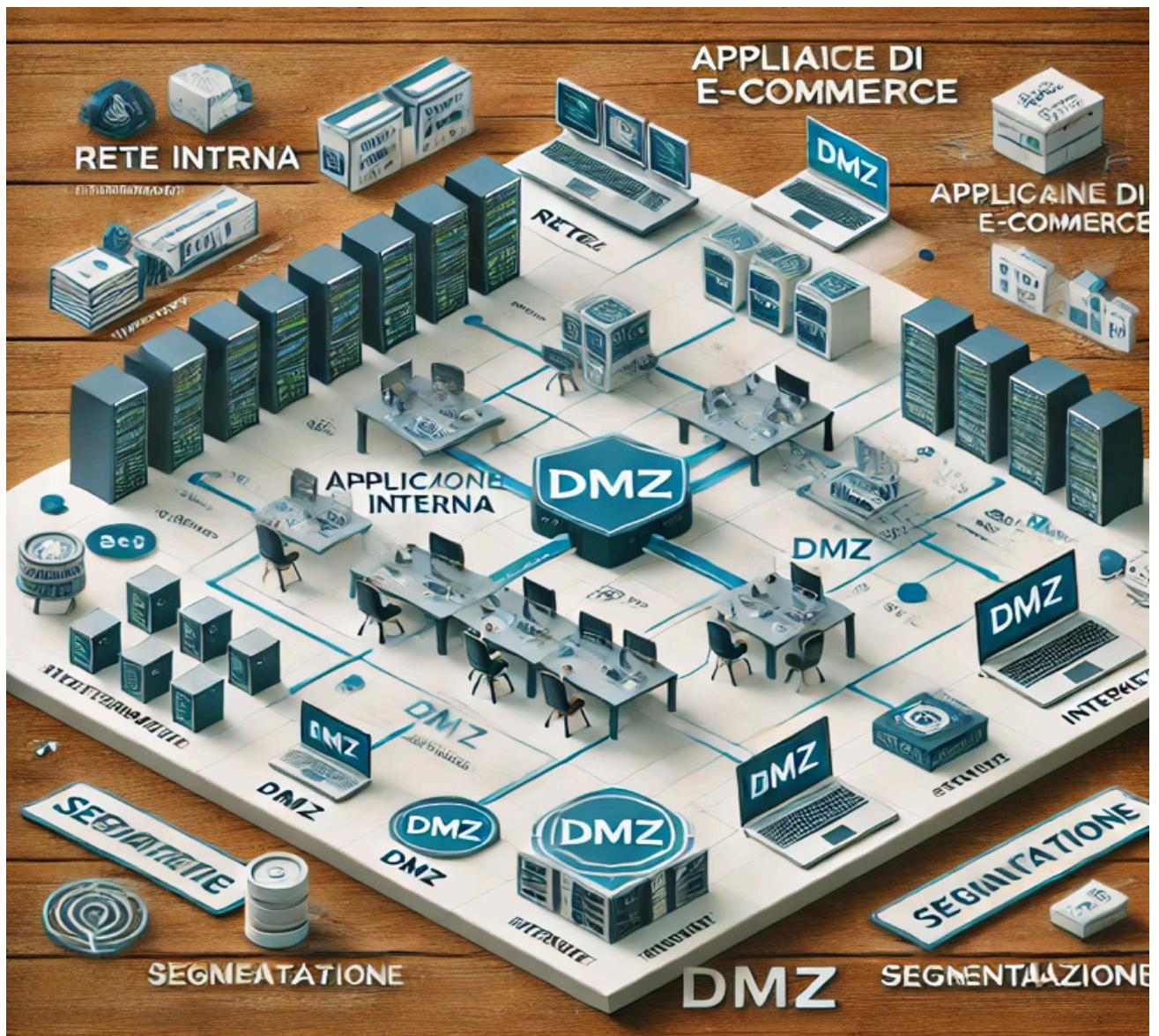
3. Risposta a un'infezione da malware

Misure di risposta:

- Segmentazione della rete: Garantire una rigorosa segmentazione della rete per prevenire la diffusione del malware dalla DMZ alla rete interna.
- Quarantena dei sistemi infetti: Isolare il sistema infetto per impedire il movimento laterale.

Modifiche alla figura:

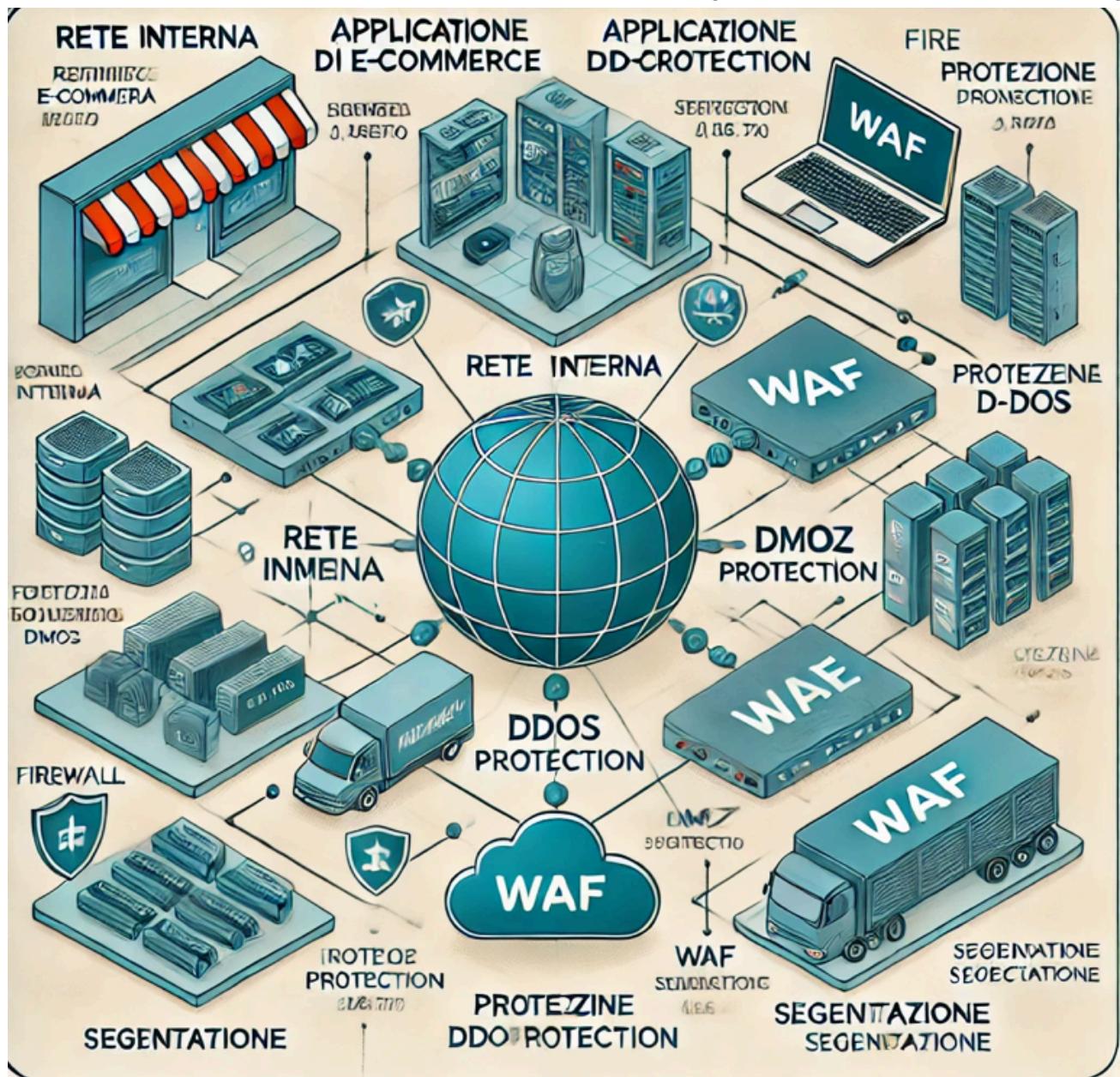
- Aggiungere misure di segmentazione e quarantena per prevenire la diffusione dalla DMZ alla rete interna.



4. Soluzione combinata per prevenzione e risposta

Modifiche alla figura:

- Combinare il WAF, la protezione DDoS e le misure di segmentazione della rete in un'unica figura.



5. Modifica “più aggressiva” per migliorare la sicurezza

Misure migliorative:

- Autenticazione Multi-Fattore (MFA): Implementare MFA per accedere sia all'applicazione di e-commerce che alla rete interna.
- Architettura Zero Trust: Adottare un modello Zero Trust per verificare rigorosamente tutte le richieste di accesso.

Modifiche alla figura:

- Includere gateway MFA e un livello di accesso Zero Trust.

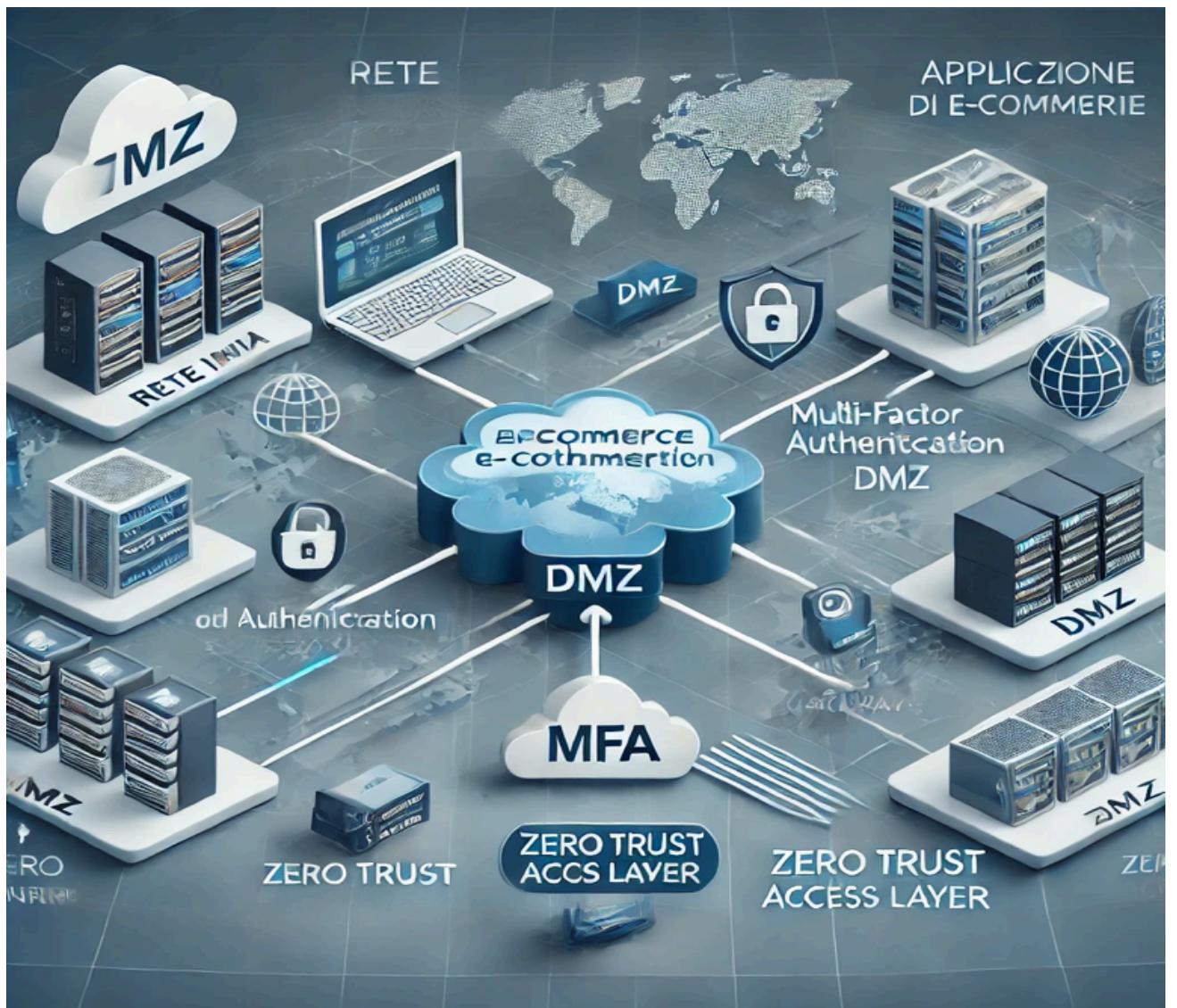


Figura combinata e migliorata

